Privacy issue for fast-track consideration by HIT Commission: Proposed Standard Consent

Prepared by

MiHIN Operations Advisory Committee (MOAC)

Privacy Working Group

October 2013

MiHIN Shared Services

Objectives

As presented at prior HIT Commission meetings:

- Develop standard for scope and type of **shareable mental health, substance abuse treatment information**
- Create **standard consent language** for exchange of Behavioral Health Information
- Support the effort to develop and pilot **use cases for sharing Behavioral Health Information (BHI)**

Consent Form Progress

- Further reviews & comments from additional parties
  - HIT Commissioners [thank you!]
  - Michigan HIMSS
  - Health Care Section of the Michigan Bar Association
  - Other Michigan stakeholders
- Coordinating with Judge Curtis Bell and the Diversions effort (need to convene both groups) & Dr. Bernie Han
- Major influencing factors on our progress:
  - Existence of two proposed standard consent forms
  - Advance of Judge Bell's proposed legislation

Judge Bell's proposed legislative amendment

Page 1

A bill to amend 1974 PA 258, entitled

"Mental health code,"

(MCL 330.1001 to 330.2106) by adding section 141a.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

SEC. 141A. (1) ON OR BEFORE JANUARY 1, 2014, THE DEPARTMENT SHALL DEVELOP A STANDARD RELEASE FORM FOR EXCHANGING CONFIDENTIAL MENTAL HEALTH INFORMATION FOR USE BY ALL PUBLIC AND PRIVATE AGENCIES, DEPARTMENTS, CORPORATIONS, OR INDIVIDUALS. ALL PARTIES DESCRIBED IN THIS SUBSECTION SHALL HONOR AND ACCEPT THE STANDARD RELEASE FORM CREATED BY THE DEPARTMENT UNDER THIS SECTION FOR THE PURPOSE FOR WHICH IT WAS CREATED.

(2) BEGINNING ON THE EFFECTIVE DATE OF THE AMENDATORY ACT THAT ADDED THIS SECTION, THE DEPARTMENT SHALL CREATE A WORKGROUP TO IMPLEMENT THE PROVISIONS OF THIS SECTION.

MiHIN Shared Services

Judge Bell's proposed legislative amendment

Page 2

(3) THE WORKGROUP CREATED IN SUBSECTION (2) SHALL MEET PERIODICALLY, AS THE DEPARTMENT CONSIDERS NECESSARY, BUT NOT LESS THAN ONCE A YEAR.

(4) IN DEVELOPING THE STANDARD RELEASE FORM UNDER SUBSECTION (1), THE DEPARTMENT SHALL CONSIDER ALL OF THE FOLLOWING:

(A) EXISTING AND POTENTIAL TECHNOLOGIES THAT COULD BE USED TO SECURELY TRANSMIT A STANDARD RELEASE FORM.

(B) THE NATIONAL STANDARDS PERTAINING TO ELECTRONIC RELEASE OF CONFIDENTIAL INFORMATION, INCLUDING PROTECTING A PATIENT'S IDENTITY AND PRIVACY IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, PUBLIC LAW 104-191.

(C) ANY PRIOR RELEASE FORMS AND METHODOLOGIES USED IN THIS STATE.

(D) ANY PRIOR RELEASE FORMS AND METHODOLOGIES DEVELOPED BY FEDERAL AGENCIES.

(5) THE STANDARD RELEASE FORM SHALL BE AVAILABLE IN BOTH ELECTRONIC AND PAPER FORM.

(6) ANY TRANSMISSION OF A STANDARD RELEASE FORM VIA ELECTRONIC MEDIA SHALL BE ACCEPTED AS AN ORIGINAL BY THE PARTY RECEIVING THE STANDARD RELEASE FORM.

Some Differences in Proposed Forms

- The MOAC Privacy Working Group form is:
  - structured to share all information once consent is obtained
  - designed primarily by CIOs, vendors, SMEs, and attorneys

- The Diversions group form:
  - has discrete categories of information that can (or cannot) be shared:

SPECIFIC INFORMATION TO BE RELEASED (Must be completed):

Yes ☐ No ☐ Assessment(s)
All ☐; General Health ☐; Mental Health ☐; Substance Abuse ☐

Yes ☐ No ☐ History & Physical Information
Yes ☐ No ☐ Operative Reports
Yes ☐ No ☐ Emergency Room Reports
Yes ☐ No ☐ Laboratory Reports
Yes ☐ No ☐ X-Ray Films and/or Radiology Reports
Yes ☐ No ☐ Consultations

  - is slightly more "plain English" for *different* reading levels

Reviewing Organizations

- Bay/Arenac Behavioral Health Authority
- Beacon
- Blue Cross Blue Shield of Michigan
- Carebridge
- Clinton- Eaton-Ingham Community Mental Health Authority
- Detroit Wayne Community Mental Health Authority
- Dickinson-Wright
- Great Lakes Health Information Exchange
- Ingenium
- Jackson Community Medical Record
- Kalamazoo Community Mental Health & Substance Abuse and Services
- Macomb County Community Mental Health Agency
- Michigan Department of Community Health
- Michigan Health & Hospital Association
- Michigan Health Connect
- Michigan Health Information Technology Commission
- MI-HIMSS
- Michigan Mental Health Diversion Council
- Michigan State Medical Society
- Netsmart
- Oakland County Community Mental Health Authority
- PCE Systems
- Provider Alliance of the Michigan Association of Community Mental Health Boards
- Southeast Michigan Health Information Exchange
- State Bar of Michigan – Health Care Section
- State of Michigan
- Summit Pointe
- The Standards Group/CIO forum
- Upper Peninsula Health Information Exchange
- Venture Behavioral Health
- Washtenaw Community Mental Health Authority

Recommendations

- The MOAC Privacy Working Group recommends:
  - Form a combined working group comprised of key individuals that have contributed to the development of both consent forms with the assignment of converging the forms into one form to be submitted to DCH *regardless of whether legislation is enacted.*
  - Insure that the Director of DCH is fully apprised and informed:
    - the pending legislation and the status quo of the legislation
    - two forms exist from parallel efforts
    - representatives from both efforts are communicating
    - both groups strongly desire to work together

Questions

Presenter

Bill Riley

Chief Information Officer at Oakland County CMH and Oakland Integrated Health Network (FQHC)

MiHIN Shared Services

CHARTERED BY THE MICHIGAN HEALTH
INFORMATION NETWORK SHARED SERVICES

MIHIN OPERATIONS ADVISORY COMMITTEE (MOAC)
PRIVACY WORKING GROUP (PWG)

Maintaining the Privacy of Health Information in Michigan's Electronic Health Information Exchange Network

Draft Privacy Whitepaper

Third Quarter 2013

This white paper is written by national and regional experts for the State of Michigan's Health Information Technology Commission, for the purpose of providing the Commission with an overview of the intersection of current privacy laws with the electronic sharing of health information in Michigan's health information exchange environment, and sets forth recommendations on steps needed to achieve a successful health information exchange in Michigan while complying with the established laws protecting individual privacy rights. Although legal issues may be discussed, this paper is not intended and should not be construed as legal advice.

Table of Contents

1. DEFINITIONS

- "**Covered Entity**" is a term used in the HIPAA Privacy Rule and means health plans, health care clearinghouses and health care providers, and is specifically defined in Section 160.103 of Subpart A of part 160 of the HIPAA Final Rules.
- "**Business Associate**" is a term used in the HIPAA Privacy Rule and generally means a person who is engaged on behalf of a Covered Entity to perform certain health care activities and functions, as specifically defined in Section 160.103 of Subpart A of part 160 of the HIPAA Final Rules.
- "**DHHS**" means the United States Department of Health & Human Services.
- "**Electronic Health Record**" or "**EHR**" means a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.
- "**HIE**" means a Health Information Exchange organization that provides services to enable the electronic sharing of health related information among Participants.
- "**HIPAA**" means the Health Insurance Portability & Accountability Act of 1996, Public Law 104-191.
- "**HIPAA Final Rules**" means the HIPAA Privacy, Security, Enforcement and Breach Notification Rules, located at 45 CFR Parts 160 and 164.
- "**HIPAA Privacy Rule**", located at 45 CFR Part 164, Subpart E, applies to Covered Entities and, where provided, Business Associates, establishing a baseline of national privacy standards with respect to PHI.
- "**HIT**" or "Health Information Technology" means technology to facilitate the electronic sharing of health-related information among organizations.
- "**HIT Commission**" means the Michigan Health Information Technology Commission that was created in May 2006 as an advisory commission to the Michigan Department of Community Health.
- "**HITECH Act**" means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Reinvestment and Recovery Act of 2009
- "**Participants**" means the organizations (such as healthcare providers) that directly or indirectly participate in the electronic exchange of health information through the HIE.
- "**Patient Identifying Information**" means for purposes of the Federal Confidentiality of Substance Abuse Records regulations, the "name, address, social security number, fingerprints, photographs of similar information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information."
- "**Patient Portal**" means a secure online website that gives patients convenient 24-hour access to personal health information from anywhere with an Internet connection. (http://www.healthit.gov/providers-professionals/faqs/what-patient-portal)
- "**Personal Health Record**" means an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. (16 CFR §318.2(d))
- "**PHI**" or "Protected health information" is a term used in the HIPAA Privacy Rule and means a subset of health information, including demographic information collected from

an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii)With respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI specifically excludes information (i) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) in employment records held by a Covered Entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.

- "**Qualified Service Organization Agreement**" means for purposes of the Federal Confidentiality of Substance Abuse Records regulations, the agreement that allows for the disclosure of Patient Identifying Information to the HIE.

2. INTRODUCTION

2.1 The Pursuit of Widespread Adoption and Use of Electronic Health Information

The stage has been set both nationally and regionally to make rapid progress on electronic health information exchange to support the three-part aim for improvement of health care in our country: better care, affordable care, and healthy people and communities.[1] Evidence suggests that one way to achieve the three-part aim is through the electronic sharing of health information among providers involved in the transitions of care and with patients and their families.[2] Information that is accurate, up to date, and available when and where a patient seeks care has been deemed the lifeblood of health care improvement and crucial to reaching these goals.[3]

The promulgation of the HITECH Act in 2009 symbolized an unprecedented investment by the Federal government in HIT for the purpose of achieving the three-part aim. Provisions of the HITECH Act were designed to establish programs that work together to provide necessary assistance and technical support to providers, enable coordination and alignment within and among states, establish connectivity to the public health community in case of emergencies, and assure the workforce is properly trained and equipped to be meaningful users of electronic health records.[4]

The HITECH Act established incentives for healthcare providers to utilize electronic health record technology. Under the "meaningful use" program of the HITECH Act, certain eligible healthcare professionals and hospitals may earn Medicare or Medicaid incentive payments if they adopt "certified EHR technology" and meaningfully use it to achieve specified

---

1 See Program Information Notice, Department of Health & Human Services, dated March 22, 2012, located at http://www.healthit.gov/sites/default/files/hie-interoperability/onc-hie-pin-003-final.pdf.

2 See Accelerating Progress: Using Health Information Technology and Electronic Health Information Exchange to Improve Care. First Annual Report and Recommendations from the State Alliance for E-Health.

3 See Program Information Notice, infra.

4 See http://www.healthit.gov/policy-researchers-implementers/health-it-adoption-programs.

objectives.[5] These objectives include, among other things, rigorous electronic exchange of health information objectives including electronic transmission of patient care summaries across multiple settings and online patient access to health information.[6] The failure to achieve meaningful use objectives within prescribed timeframes will result in the assessment of penalties against these providers starting in 2014.

Michigan has made significant progress in facilitating the adoption and use of electronic health information exchange within the state. Under the HITECH Act's State HIE Cooperative Agreement, Michigan was awarded $14.9 million in Federal grants to assist with achieving statewide electronic exchange of health information.[7] The Michigan HIT Commission has implemented measures and achieved significant progress in the state-wide adoption of electronic health records, the promotion of electronic HIE, and the increased utilization of other types of HIT such as the use of patient registries and electronic prescribing.[8] The HIT Commission has been charged with, among other things, developing and maintaining a strategic plan for the HIE to include measures to protect the privacy and security of health information transmitted through the HIE,[9] and Michigan Health Information Network Shared Services was created in 2010 to administer the technical and business operations of Michigan's State HIE Cooperative Agreement program.

While this White Paper focuses on the impact that privacy laws have on HIE operations, the security of health information transmitted in the HIE is equally important.[10] The two concepts, although distinct, are related, and both must be considered in the context of establishing public trust and confidence in the protection of health information transmitted through HIEs. We cannot have privacy without security. The privacy of health information focuses on the "what" and "whose" information is protected and the right of an individual to control the use of his or her information. The security of health information focuses on the "how" that information is protected, including through administrative, technical and physical safeguards such as encryption. This White Paper should therefore be read in conjunction with the "Health Information & Cyber Security In Michigan" White Paper distributed to the HIT Commission during the first quarter of 2013.

2.2 The Application of Privacy Laws to HIE Operations

There exists a natural tension between the free and efficient exchange of health information and the myriad federal and state privacy laws governing such information. HIEs and their Participants must understand and comply with all laws and regulations protecting individual privacy rights in the transmission and use of health information. Demonstrated compliance is critical in securing the public's trust and confidence in the electronic sharing of health information.

---

5 See the Centers for Medicare & Medicaid Services website, located at http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html (last accessed August 28, 2013).

6 See id.

7 See http://www.healthit.gov/policy-researchers-implementers/state-health-information-exchange.

8 See the Michigan Health Information Technology Commission website, located at http://www.michigan.gov/mdch/0,1607,7-132-2946_44257---,00.html, last visited August 24, 2013.

9 See MCLA § 333.2505(2)(d).

10 See Security White Paper.

The following federal laws, rules and regulations govern the privacy of certain types of health information, including PHI:

- The HIPAA Privacy Rule establishes a baseline of national privacy standards solely with respect to Protected Health Information. Relevant considerations for HIEs and their Participants under the HIPAA Privacy Rule include:
  - Business Associate. Absent extraordinary circumstances, HIEs will be deemed "business associates" having direct liability under HIPAA for uses and disclosures of PHI, including electronic PHI. Participants may be business associates vis-à-vis other Participants, depending on the nature of services provided and PHI received in support of those services.
  - Notice of Privacy Practices. Covered Entities having direct treatment relationships with individuals must provide a copy of their HIPAA-compliant Notice of Privacy Practices, describing, among other things, how a Covered Entity may use and disclose their PHI, the individuals' rights with respect to that information, as well as the Covered Entity's obligations to protect the information.
  - Patient Authorizations. A Covered Entity must obtain an individual's written authorization (in a HIPAA-compliant format) for any use or disclosure of PHI that is not for "treatment, payment or health care operations" or otherwise permitted or required by the HIPAA Privacy Rule. Additionally, a Covered Entity must obtain an individual's written authorization to use and disclose psychotherapy notes for treatment, payment and health care operations, with limited exceptions.
- Family Educational Rights & Privacy Act, at 20 U.S.C. § 1232g, protects the privacy of information maintained in student education records, which includes student health records. HIPAA specifically excludes information subject to FERPA from the definition of PHI.
- The Confidentiality of Alcohol and Drug Abuse Patient Records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR Part 2, imposes special restrictions upon the disclosure and use of alcohol and drug abuse patient records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program.
- The Clinical Laboratory Improvement Amendments, at 42 CFR § 493.1291(f), prohibits the disclosure of laboratory test results except to authorized persons, and if applicable the individual responsible for using the test results and the laboratory that initially requested the test.

The following State of Michigan laws govern the privacy of certain types of health information:

- Mental Health Records. The Michigan Mental Health Code, at MCLA §§ 333.1748 and 333.1748a, sets forth very limited circumstances under which mental health records may be disclosed without consent. These generally include disclosures mandated by legal process, or in conjunction with a child neglect or child abuse investigation.

- Serious Communicable Diseases. The Michigan Public Health Code, at MCL § 333.5131, 5114a, specifically requires that all reports, records and data pertaining to testing, care, treatment, reporting and research, and information pertaining to partner notification, that are associated with the serious communicable diseases or infections of HIV and acquired immunodeficiency syndrome be kept confidential, and may be disclosed only in very limited situations.
- Abortions. The Michigan Public Health Code, at MCL § 333.2835, requires that reports of abortions be kept confidential, permitting disclosure in very limited circumstances.
- Records of Minors. The Michigan Medical Records Access Act, at MCL § 333.26263, provides that in the event a minor lawfully obtained healthcare without the consent or notification of a parent, guardian or other person acting in loco parentis, the minor has the exclusive right to exercise the rights of a patient with respect to medical records relating to that care.

The types of health information covered by the non-HIPAA laws and regulations described above are referred to herein as "other health information," or "OHI."

2.3 The Importance of Patient Consent Management

The HIPAA Privacy Rule generally permits PHI to be used and disclosed for treatment (as well as payment and health care operations) without the patient's written authorization (with the express exception of psychotherapy notes). Various federal and state laws governing OHI, however, adopt more stringent requirements for disclosure and use, often mandating written patient consent to disclose even for treatment purposes.[11] These differing consent requirements have been identified as potential impediments to the electronic exchange of health information[12], and surveys indicate that states find the process of electronically implementing permission requirements within an HIE to be confusing.[13]

Facilitating the disclosure of PHI *and* OHI through an HIE is important to the overall goal of achieving coordination of care. Studies have shown that people with certain behavioral or mental health disorders die at a younger age or have higher rates of chronic life-threatening conditions than those in the general population, and that a major reason for this is their lack of contact with primary care services.[14] HIEs must therefore ensure that they and their Participants adopt and implement protocols, including consent forms that enable the exchange of PHI and OHI in compliance with patients' privacy rights.

---

[11] See 45 C.F.R. § 164.506(c)

[12] See Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Law Requirements for Patient Permission to Disclose Health Information, dated August 2009, located at http://www.healthit.gov/sites/default/files/disclosure-report-1.pdf (last access August 29, 2013).

[13] See id.

[14] See "Understanding Health Reform: Integrated Care and Why You Should Care" Substance Abuse and Mental Health Services Administration, located at http://www.samhsa.gov/healthReform/docs/ConsumerTipSheet_IntegrationImportance.pdf (last accessed August 29, 2013).

As an example, the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations allow disclosures of Patient Identifying Information by an alcohol and drug program only with the patient's prior written consent, in a medical emergency, or when the program has signed Qualified Service Organization/Business Associate Agreements with the recipient of the information. Furthermore, any authorized disclosure must include a statement that the information disclosed is protected by federal law and that the recipient may not make any further disclosure of it unless permitted by the regulations. An HIE and its Participants must therefore develop procedures to verify that (i) the patient's prior written consent exists and covers the intended disclosure, and (ii) the required notice is delivered to and received by the recipient.

Finally, the continuing development of Patient Portals and the Personal Health Record industry suggest that HIEs and their Participants should consider developing a consent management process that covers permissions necessary with respect to the transfer of Patient Portal data through the HIE. In particular, these consents should address family and friends' access to data through the Patient Portals.

2.4 Overall Issue Statement

Tensions exist between federal and state laws established to protect the privacy of health information and the goal of rapid and widespread adoption of electronic health information exchange, resulting in complexities that must be fully understood and effectively addressed in the HIE environment and infrastructure.

3. OPPORTUNITY FOR PROACTIVE ACTION

This document is meant to serve as an outline of high level privacy-related recommendations from national and regional experts to the Michigan Health Information Technology (HIT) Commission. The HIT Commission was created by PA 137-06. The HIT Commission is housed within the Michigan Department of Community Health and its commissioners are appointed by the governor. The HIT Commission's mission is to facilitate and promote the design, implementation, operation, and maintenance of an interoperable health care information infrastructure in Michigan. The 13-member HIT Commission was appointed in August 2006 and met for the first time in October 2006. It is anticipated that the HIT Commission will employ this report as a proactive vehicle to fulfill its mission and ensure that patients, providers, and policymakers in Michigan can remain confident that health information is protected and accessed appropriately when shared electronically as more and more providers adopt new forms of HIT.

The origin of this White Paper is the MiHIN Operations Advisory Committee (MOAC) Security and Privacy Working Group (S&P WG) which focused on Cyber Security in 2012 and presented a Cyber Security White Paper to the HIT Commission in January 2013. Simultaneously in January 2013 the S&P WG spun off its first Privacy Work Shop in Lansing in January 2013 followed by a second Privacy Workshop in April 2013. These workshops accomplished several things. First, the workshops produced areas of concern in Privacy where work would be needed to remedy known or looming issues.

At the April workshop, one particular issue was identified as needing urgent attention and was deemed a "fast track" issue – the need for a statewide standard consent form, standard consent language, and consent use cases for behavioral health, which is an opt-in, as opposed to physical health, which is an opt-out. The "fast track" behavioral health standard consent issue was presented to the HIT Commission at its July 2013 meeting and is on a separate, parallel track to this White Paper effort. The initial draft standard consent materials are planned to be presented at the September 19, 2013 HIT Commission meeting.

Also, it became clear that the MOAC Security & Privacy Working Group should spin off Privacy into a separate Working Group. The new MOAC Privacy Working Group has been drafting and reviewing this White Paper since April and is now ready to begin the external review process as described later herein. The major areas of recommendations on privacy will now be described.

4. PRIVACY AWARENESS & EDUCATION AREAS

HIEs and their Participants engaged in the exchange of PHI and OHI must have full awareness of all implicated privacy laws and regulations, and adopt policies and procedures to ensure compliance with those laws and regulations. As a consequence, the MOAC Privacy Working Group recommends the following:

4.1 Direct an entity designated by the State to develop an education and training program with a privacy awareness curriculum to provide organizations that exchange health information with a clear understanding of their privacy obligations and the need for policies and procedures designed to meet those obligations. Coordinate this training with training targeted at security awareness.

4.2 Direct an entity designated by the State to develop an attestation document for organizations to affirm that comprehensive privacy policies and procedures have been documented, adopted, implemented, and enforced.

4.3 Direct an entity designated by the State to develop and conduct an auditing program to confirm that organizations engaged in health information exchange have adopted and properly implemented policies and procedures for compliance with applicable privacy laws and regulations.

5. RISK IDENTIFICATION AND MANAGEMENT

In order to effectively promote the inclusion of OHI and Patient Health Records in the universe of exchanged information, HIEs and Participants must understand and accept the risks attendant to the exchange of these classes of information. HIEs and Participants need to understand their own responsibilities and proscribed actions, as well the reassurance that the other Participants will act as expected in the event of a privacy event (unauthorized disclosure). As a consequence, the MOAC Privacy Working Group recommends the following:

5.1 Clarify the nature of the legal risks associated with a violation of each pertinent privacy law or regulation, and their potential application to an HIE or a Participant.

5.2 Direct an entity designated by the State to provide guidance regarding existing or recommended federal and state "safe harbor" conditions that may apply to the operations of HIEs and that may insulate HIEs, Participants, or both from liability under applicable privacy laws and regulations.

5.3 Direct an entity designated by the State to provide guidance as to when HIEs must respond to violations of privacy laws that are known to the HIE, or that are disclosed by HIE Participants, and create standardized responses that should be used by HIEs in such event.

5.4 Direct an entity designated by the State to determine the terms and conditions for data exchange between the HIEs and the Veteran's Administration and other Federal entities.

6. PATIENT CONSENT AND AUTHORIZATION

Consent management is fundamental to the introduction of PHI and OHI into and HIE environment. HIEs, Participants, and the public must have confidence that required consents and authorizations have been obtained for all health information transmitted through the HIE. The development and implementation of an effective and efficient consent management HIE regime requires substantial support from all HIE stakeholders. As a consequence, the MOAC Privacy Working Group recommends the following:

6.1 Direct an entity designated by the State to determine the specific consent/authorization rules with respect to the transmission of PHI, each type of OHI, or Patient Health Records.

6.2 Direct an entity designated by the State to create a standard framework around the transmission of PHI and each type of OHI through the HIE that is consistent with the rules identified in Section 5.1, and the HIE's role with respect to facilitating the framework. This might include the development of standard consent forms to be used by Participants (e.g., "all-in", "all-out", and "check the box" consents).

6.3 Direct an entity designated by the State to investigate and recommend a technical framework/architecture to enable the implementation of the adopted consent regime. This might include investigation into the necessity of data segmentation in HIEs relating to OHI *(or what information must be defined for data segmentation)* and the appropriate methods to effectuate such data segmentation.

7. CONTRIBUTORS

We wish to express our appreciation to the many contributors who co-authored, reviewed and responded to the recommendation prioritization survey to support the development of this White Paper:

Bay/Arenac Behavioral Health Authority
Beacon
Blue Cross Blue Shield of Michigan
Carebridge
Clinton- Eaton-Ingham Community Mental Health Authority

Detroit Wayne Community Mental Health Authority
Dickinson-Wright
Great Lakes Health Information Exchange
Ingenium
Jackson Community Medical Record
Kalamazoo Community Mental Health & Substance Abuse and Services
Macomb County Community Mental Health Agency
Michigan Department of Community Health
Michigan Health & Hospital Association
Michigan Health Connect
Michigan Health Information Technology Commission
MI-HIMSS
Michigan Mental Health Diversion Council
Michigan State Medical Society
Netsmart
Oakland County Community Mental Health Authority
PCE Systems
Provider Alliance of the Michigan Association of Community Mental Health Boards
Southeast Michigan Health Information Exchange
State Bar of Michigan
State of Michigan
Summit Pointe
The Standards Group/CIO forum
Upper Peninsula Health Information Exchange
Venture Behavioral Health
Washtenaw Community Mental Health Authority

BLOOMFIELD 50913-2 1331282vI